UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/071,228 | 02/08/2002 | Steven A. Pettit | ENB-012(E00378/70181) | 9237 |

959 7590 12/13/2005

LAHIVE & COCKFIELD, LLP.
28 STATE STREET
BOSTON, MA 02109

| EXAMINER | |
|---|---|
| WONG, WARNER | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2668 | |

DATE MAILED: 12/13/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 10/071,228 | PETTIT ET AL. | |
| | Examiner | Art Unit | |
| | Warner Wong | 2668 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *08 February 2002*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-40* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-40* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *08 February 2002* is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

## DETAILED ACTION

### *Specification*

1. Applicant is reminded of the proper language and format for an abstract of the disclosure.

The abstract should be in narrative form and generally limited to a single paragraph on a separate sheet within the range of 50 to 150 words. It is important that the abstract not exceed 150 words in length since the space provided for the abstract on the computer tape used by the printer is limited.

### *Claim Objections*

The following claims are objected to because of the following informalities:

2. Claim 7, line 4: The phrase "one more" should be grammatically corrected to "one or more".

3. Claim 19, line 4: The phrase "one more" should be grammatically corrected to "one or more".

4. Claim 39, line 8: The limitation "service abstraction" is not defined in (this) independent claim.

5. Claim 39, line 8: The phrase "one more" should be grammatically corrected to "one or more".

6. Claim 40, line 11: The limitation "service abstraction" is not defined in (this) independent claim.

7. Claim 40, line 11: The phrase "one more" should be grammatically corrected to "one or more".

Appropriate correction is required.

***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

1. Claims 1-3 and 5-6 are rejected under 35 U.S.C. 102(e) as being anticipated by See (2003/0021283).

**Regarding claim 1**, See describes a system of controlling usage of network resources on a communication network, comprising:

(A) creating one or more packet rules (policy rules) for analyzing packets received at one or more devices of the communications network, each rule including a condition and action to be taken if a packet received at a device satisfies the condition (fig. 4 and paragraph 35);

(B) creating one or more service abstractions (policy groups), each service abstraction representing a [named] set of one or more of the packet rules (paragraph 35, "According to one embodiment, the policy rules are organized into policy groups based on a rule type 52".

**Regarding claim 2**, See describes all limitations set forth in claim 1. See further describes:

(C) configuring a network device of the communications network with one or more packet rules according to at least one of the service abstractions (policy groups) (paragraph 26, "The policy repository 22 stores a plurality of policy rules that may be used by the network devices 24, 26, 28 to control different network elements" and paragraph 38, "The action 58 may be identifying a policy group based on a device attribute..")

**Regarding claim 3**, See describes all limitations set forth in claim 2. See further describes:

configuring a port module of a switching device of the communications network with one or more packet rules according to at least one of the service abstractions (paragraph 22, "According to one embodiment, the network policies are used to .. disable network ports based on predetermined conditions,")

**Regarding claim 5**, See describes all limitations set forth in claim 1. See further describes:

(C) distributing the one or more service abstractions to one or more network devices residing on the communications network (paragraph 30, "According to one embodiment, the policies relevant to a particular network device 24, 26, 28 are selected based on a role assigned to the device" and paragraph 35, "A rule type may organize policies into role policies").

**Regarding claim 6**, See describes all limitations set forth in claim 1. See further describes:

(C) associating one or more of the service abstractions with a user (computer host) of the communications network (paragraph 27, where network devices may be computer hosts, and paragraph 30, "According to one embodiment, the policies relevant to a particular network device 24, 26, 28 are selected based on a role assigned to the device" and paragraph 35, "A rule type may organize policies into role policies").

***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

**(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.**

1. **Claim 4** rejected under 35 U.S.C. 103(a) as being unpatentable over See in view of Nessett (5,968,176).

See describes all limitations set forth in claim 2. See further describes that the network devices may be gateways devices such as hubs, bridges, routers, switches (paragraph 27). See lacks what Nessett specifically describes:

configuring a firewall of a network device of the communications network with one or more packet rules according to at least one of the service abstractions (abstract, where the network devices incorporate firewall functionality).

It would have been obvious to one with ordinary skill in the art at the time of invention by applicant to specify firewall (functionality) in network devices. The motivation being that firewall functionality is a common yet important aspect to an overall (private) network for security (Nessett, col. 2, lines 9-11, "Traditionally, firewalls are implemented as border equipment, such as routers and application proxy gateways that protect a private network from external attack.)

2. Claim 7-9, and 11-12, 27-29 and 31-32 are rejected under 35 U.S.C. 103(a) as being unpatentable over See in view of Azarmi (5,905,715).

**Regarding claim 7**, See describes all limitations set forth in claim 1. See lacks what Azarmi describes:

(C) creating one or more role abstractions (feature-describing data set), each role abstraction representing a role of a user with respect to the communications network (manageable aspect of the communications network), and each role abstraction including a set of one more service abstractions (management rule profiles) (col. 2, lines 42-51).

It would have been obvious to one with ordinary skill in the art at the time of invention by applicant to specify (another) role abstraction layer to group the (existing) service abstraction layer. The motivation being that "It defines a structural architecture within which business processes, and therefore management systems required to provide services on a network", Azarmi, col. 2, lines 10-12.

**Regarding claim 8**, See and Azarmi combined describes all limitations set forth in claim 7. See and Azarmi further describe:

(D) configuring a network device of the communications network with one or more packet rules according to one of the role abstractions (See, paragraph 26, "The policy repository 22 stores a plurality of policy rules that may be used by the network devices 24, 26, 28 to control different network elements" and See, paragraph 38, "The action 58 may be identifying a policy group based on a device attribute.." *where the policy group [i.e. service abstraction layer] is replaced by Azarmi's feature set [i.e. role abstraction layer]*).

**Regarding claim 9**, See and Azarmi combined describe all limitations set forth in claim 8. See and Azarmi further describe:

configuring a port module of a switching device of the communications network with one or more packet rules according to at least one of the role abstractions (See, paragraph 22, "According to one embodiment, the network policies are used to .. disable network ports based on predetermined conditions", *where the policy (group) [i.e. service abstraction layer] is replaced by Azarmi's feature set [i.e. role abstraction layer]*).

**Regarding claim 11**, See and Azarmi combined describe all limitations set forth in claim 7. See and Azarmi further describe:

(D) distributing the one or more role abstractions to one or more network devices residing on the communications network (See, paragraph 30, "According to one embodiment, the policies relevant to a particular network device 24, 26, 28 are selected based on a role assigned to the device" and See, paragraph 35, "A rule type may

organize policies into role policies", *where the role (policy) [i.e. service abstraction layer] is replaced by Azarmi's feature set [i.e. role abstraction layer]*).

**Regarding claim 12**, See and Azarmi combined describe all limitations set forth in claim 7. See and Azarmi further describe:

(D) associating one or more of the role abstractions with a user (computer host) of the communications network (paragraph 27, where network devices may be computer hosts, and paragraph 30, "According to one embodiment, the policies relevant to a particular network device 24, 26, 28 are selected based on a role assigned to the device" and paragraph 35, "A rule type may organize policies into role policies", *where the role (policy) [i.e. service abstraction layer] is replaced by Azarmi's feature set [i.e. role abstraction layer]*).

**Regarding claims 27**, See describes a system of controlling usage of network resources on a communication network, comprising:

(A) creating one or more packet rules (policy rules) for analyzing packets received at one or more devices of the communication network, each rule including a condition and action to be taken if a packet received at a device satisfies the condition (fig. 4 and paragraph 35);

See lacks what Azarmi describes:

(B) creating one or more role abstractions (feature-describing data set), each role abstraction representing a role of a user with respect to the communications network (manageable aspect of the communications network), and each role abstraction

including a set of one more packet rule (management rule profiles containing management rules) (col. 2, lines 42-51).

It would have been obvious to one with ordinary skill in the art at the time of invention by applicant to specify the role abstraction layer to group the packet rules (layer). The motivation being that "It defines a structural architecture within which business processes, and therefore management systems required to provide services on a network", Azarmi, col. 2, lines 10-12.

**Regarding claim 28**, See and Azarmi combined describes all limitations set forth in claim 27. See and Azarmi further describe:

(C) configuring a network device of the communications network with one or more packet rules according to one of the role abstractions (See, paragraph 26, "The policy repository 22 stores a plurality of policy rules that may be used by the network devices 24, 26, 28 to control different network elements" and See, paragraph 38, "The action 58 may be identifying a policy group based on a device attribute.." *where the policy group [i.e. service abstraction layer] is replaced by Azarmi's feature set [i.e. role abstraction layer]*).

**Regarding claim 29**, See and Azarmi combined describe all limitations set forth in claim 28. See and Azarmi further describe step (C) of:

configuring a port module of a switching device of the communications network with one or more packet rules according to at least one of the role abstractions (See, paragraph 22, "According to one embodiment, the network policies are used to ..

disable network ports based on predetermined conditions", *where the policy (group) [i.e. service abstraction layer] is replaced by Azarmi's feature set [i.e. role abstraction layer]*).

**Regarding claim 31**, See and Azarmi combined describe all limitations set forth in claim 27. See and Azarmi further describe step (C) of:

(C) distributing the one or more role abstractions to one or more network devices residing on the communications network (See, paragraph 30, "According to one embodiment, the policies relevant to a particular network device 24, 26, 28 are selected based on a role assigned to the device" and See, paragraph 35, "A rule type may organize policies into role policies", *where the role (policy) [i.e. service abstraction layer] is replaced by Azarmi's feature set [i.e. role abstraction layer]*).

**Regarding claim 32**, See and Azarmi combined describe all limitations set forth in claim 27. See and Azarmi further describe:

(C) associating one or more of the role abstractions with a user (computer host) of the communications network (paragraph 27, where network devices may be computer hosts, and paragraph 30, "According to one embodiment, the policies relevant to a particular network device 24, 26, 28 are selected based on a role assigned to the device" and paragraph 35, "A rule type may organize policies into role policies", *where the role (policy) [i.e. service abstraction layer] is replaced by Azarmi's feature set [i.e. role abstraction layer]*).

3. **Claims 10 and 30** are rejected under 35 U.S.C. 103(a) as being unpatentable over See in view of Azarmi and further in view of Nessett.

**Regarding claim 10**, See and Azarmi combined describe all limitations set forth in claim 8. See further describes that the network devices may be gateways devices such as hubs, bridges, routers, switches (paragraph 27). See and Azarmi lack what Nessett specifically describes:

configuring a firewall of a network device of the communications network with one or more packet rules according to at least one of the role abstractions (abstract, where the network devices incorporate firewall functionality).

It would have been obvious to one with ordinary skill in the art at the time of invention by applicant to specify firewall (functionality) in network devices. The motivation being that firewall functionality is a common yet important aspect to an overall (private) network for security (Nessett, col. 2, lines 9-11, "Traditionally, firewalls are implemented as border equipment, such as routers and application proxy gateways that protect a private network from external attack.)

**Regarding claim 30**, See and Azarmi combined describe all limitations set forth in claim 28. See further describes that the network devices may be gateways devices such as hubs, bridges, routers, switches (paragraph 27). See and Azarmi lack what Nessett specifically describes:

configuring a firewall of a network device of the communications network with one or more packet rules according to at least one of the role abstractions (abstract, where the network devices incorporate firewall functionality).

It would have been obvious to one with ordinary skill in the art at the time of invention by applicant to specify firewall (functionality) in network devices. The

motivation being that firewall functionality is a common yet important aspect to an overall (private) network for security (Nessett, col. 2, lines 9-11, "Traditionally, firewalls are implemented as border equipment, such as routers and application proxy gateways that protect a private network from external attack.)

4. Claims 13-18 and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over See in view of Nessett.

**Regarding claims 13 and 25**, See describes a system for controlling usage of network resources on a communications network, the system comprising:

creating one or more packet rules for analyzing packets received at one or more devices of the communications network, each rule including a condition and action to be taken if a packet received at a device satisfies the condition; and

creating one or more service abstractions, each service abstraction representing a named set of one or more of the packet rules.

See lacks what Nessett describes:

a rule editing module [to create pack rules] (fig. 1, security policy management back-end #32) and a service editing module [means to create service abstractions] (fig. 1, security policy language interpreter #34)

It would have been obvious to one with ordinary skill in the art at the time of invention by applicant to specify respective editing modules to be used for creating the packet rules and service abstractions as specified in See. The motivation for using separate modules in performing layered rules & service abstraction functionality is "As

the partitioning becomes finer grained, access to resources outside of the firewall partition experiences increasing degraded performance. Another approach to this problem is to distribute firewall functionality down into lower layers of the protocol hierarchy" (Nessett, col. 2, lines 51-56).

**Regarding claim 14,** See and Nessett combined describe all limitations set forth in claim 13. See further describes:

[logic to] configure a network device of the communications network with one or more packet rules according to at least one of the service abstractions (policy groups) (paragraph 26, "The policy repository 22 stores a plurality of policy rules that may be used by the network devices 24, 26, 28 to control different network elements" and paragraph 38, "The action 58 may be identifying a policy group based on a device attribute..")

**Regarding claim 15**, See and Nessett combined describe all limitations set forth in claim 14. See further describes:

[port configuration logic ] to configure a port module of a switching device with one or more packet rules according to at least one of the service abstractions (paragraph 22, "According to one embodiment, the network policies are used to .. disable network ports based on predetermined conditions,")

**Regarding claim 16**, See and Nessett combined describe all limitations set forth in claim 14. Nessett further describes:

[firewall logic to] configure a firewall of a network device with one or more packet rules according to at least one of the service abstractions (abstract, where the network devices incorporate firewall functionality).

**Regarding claim 17**, See and Nessett combined describe all limitations set forth in claim 13. See further describes:

a distribution module (fig. 2, policy repository #20) to distribute the one or more service abstractions to one or more network devices residing on the communications network (paragraph 30, "According to one embodiment, the policies relevant to a particular network device 24, 26, 28 are selected based on a role assigned to the device" and paragraph 35, "A rule type may organize policies into role policies").

**Regarding claim 18**, See describes all limitations set forth in claim 13. See further describes:

[assigning logic to] associate one or more of the service abstractions with a user (computer host) of the communications network (paragraph 27, where network devices may be computer hosts, and paragraph 30, "According to one embodiment, the policies relevant to a particular network device 24, 26, 28 are selected based on a role assigned to the device" and paragraph 35, "A rule type may organize policies into role policies").

5. Claims 19-24 and 33-40 are rejected under 35 U.S.C. 103(a) as being unpatentable over See in view of Nessett and further in view of Azarmi.

**Regarding claim 19**, See and Nessett combined describe all limitations set forth in claim 13. See and Nessett lacks what Azarmi describes:

A role editing module (Nessett, fig. 1, front end #31) to create one or more role abstractions (feature-describing data set), each role abstraction representing a role of a user with respect to the communications network (manageable aspect of the communications network), and each role abstraction including a set of one more service abstractions (management rule profiles) (col. 2, lines 42-51).

It would have been obvious to one with ordinary skill in the art at the time of invention by applicant to specify (another) role abstraction layer to group the (existing) service abstraction layer. The motivation being that "It defines a structural architecture within which business processes, and therefore management systems required to provide services on a network", Azarmi, col. 2, lines 10-12.

**Regarding claim 20**, See, Nessett and Azarmi combined describe all limitations set forth in claim 19. See, Nessett and Azarmi further describe:

[logic to] configure a network device with one or more packet rules according to one of the role abstractions (See, paragraph 26, "The policy repository 22 stores a plurality of policy rules that may be used by the network devices 24, 26, 28 to control different network elements" and See, paragraph 38, "The action 58 may be identifying a policy group based on a device attribute.." *where the policy group [i.e. service abstraction layer] is replaced by Azarmi's feature set [i.e. role abstraction layer]*).

**Regarding claim 21**, See, Nessett and Azarmi combined describe all limitations set forth in claim 20. See, Nessett and Azarmi further describe:

[port configuration logic to] configure a port module of a switching device with one or more packet rules according to one of the role abstractions (See, paragraph 22,

"According to one embodiment, the network policies are used to .. disable network ports based on predetermined conditions", *where the policy (group) [i.e. service abstraction layer] is replaced by Azarmi's feature set [i.e. role abstraction layer]*).

**Regarding claim 22**, See, Nessett and Azarmi combined describe all limitations set forth in claim 20. Nessett further describe:

[firewall logic to] configure a firewall of a network device with one or more packet rules according to one of the role abstractions (abstract, where the network devices incorporate firewall functionality).

**Regarding claim 23**, See, Nessett and Azarmi combined describe all limitations set forth in claim 19. See, Nessett and Azarmi further describe:

a distribution module (See, fig. 2, policy repository #20) to distribute the one or more role abstractions to one or more network devices residing on the communications network (See, paragraph 30, "According to one embodiment, the policies relevant to a particular network device 24, 26, 28 are selected based on a role assigned to the device" and See, paragraph 35, "A rule type may organize policies into role policies", *where the role (policy) [i.e. service abstraction layer] is replaced by Azarmi's feature set [i.e. role abstraction layer]*).

**Regarding claim 24**, See and Azarmi combined describe all limitations set forth in claim 19. See and Azarmi further describe:

[assigning logic to] assign one of the role abstractions to a [first] user (computer host) of the communications network (paragraph 27, where network devices may be computer hosts, and paragraph 30, "According to one embodiment, the policies relevant

to a particular network device 24, 26, 28 are selected based on a role assigned to the device" and paragraph 35, "A rule type may organize policies into role policies", *where the role (policy) [i.e. service abstraction layer] is replaced by Azarmi's feature set [i.e. role abstraction layer]*).

**Regarding claims 33 and 39-40**, See describes a system of controlling usage of network resources on a communication network [official notice taken that the system may be implemented using a computer comprising a readable medium and a program with instructions which executes the process], comprising:

creating one or more packet rules (policy rules) for analyzing packets received at one or more devices of the communication network, each rule including a condition and action to be taken if a packet received at a device satisfies the condition (fig. 4 and paragraph 35);

See lacks what Azarmi describes:

creating one or more role abstractions (feature-describing data set), each role abstraction representing a role of a user with respect to the communications network (manageable aspect of the communications network), and each role abstraction including a set of one more packet rule (management rule profiles containing management rules) (col. 2, lines 42-51).

It would have been obvious to one with ordinary skill in the art at the time of invention by applicant to specify the role abstraction layer to group the packet rules (layer). The motivation being that "It defines a structural architecture within which

business processes, and therefore management systems required to provide services on a network", Azarmi, col. 2, lines 10-12.

See and Azarmi combined lack what Nessett describes:

a rule editing module [to create pack rules] (fig. 1, security policy management back-end #32) and a role editing module (Nessett, fig. 1, front end #31) [means to create role abstractions].

It would have been obvious to one with ordinary skill in the art at the time of invention by applicant to specify respective editing modules to be used for creating the packet rules and service abstractions as specified in See and Arzarmi. The motivation for using separate modules in performing layered rules & service abstraction functionality is "As the partitioning becomes finer grained, access to resources outside of the firewall partition experiences increasing degraded performance. Another approach to this problem is to distribute firewall functionality down into lower layers of the protocol hierarchy" (Nessett, col. 2, lines 51-56).

**Regarding claim 34**, See, Nessett and Azarmi combined describe all limitations set forth in claim 33. See, Nessett and Azarmi further describe:

[logic to] configure a network device of the communications network with one or more packet rules according to one of the role abstractions (See, paragraph 26, "The policy repository 22 stores a plurality of policy rules that may be used by the network devices 24, 26, 28 to control different network elements" and See, paragraph 38, "The action 58 may be identifying a policy group based on a device attribute.." *where the*

*policy group [i.e. service abstraction layer] is replaced by Azarmi's feature set [i.e. role abstraction layer]*).

**Regarding claim 35**, See, Nessett and Azarmi combined describe all limitations set forth in claim 34. See, Nessett and Azarmi further describe step (C) of:

[port configuration logic] to configure a port module of a switching device of the communications network with one or more packet rules according to at least one of the role abstractions (See, paragraph 22, "According to one embodiment, the network policies are used to .. disable network ports based on predetermined conditions", *where the policy (group) [i.e. service abstraction layer] is replaced by Azarmi's feature set [i.e. role abstraction layer]*).

**Regarding claim 36**, See, Nessett and Azarmi combined describe all limitations set forth in claim 34. See, Nessett and Azarmi further describe:

[firewall logic] to configure a firewall of a network device of the communications network with one or more packet rules (Nessett, abstract, where the network devices incorporate firewall functionality) [according to one of the role abstractions].

**Regarding claim 37**, See, Nessett and Azarmi combined describe all limitations set forth in claim 33. See, Nessett and Azarmi further describe step (C) of:

a distribution module (See, fig. 2, #20) to distribute one or more role abstractions to one or more network devices residing on the communications network (See, paragraph 30, "According to one embodiment, the policies relevant to a particular network device 24, 26, 28 are selected based on a role assigned to the device" and See, paragraph 35, "A rule type may organize policies into role policies", *where the role*

*(policy) [i.e. service abstraction layer] is replaced by Azarmi's feature set [i.e. role abstraction layer]*).

**Regarding claim 38**, See, Nessett and Azarmi combined describe all limitations set forth in claim 33. See, Nessett and Azarmi further describe:

[assigning logic to] assign one or more of the role abstractions with a user (computer host) of the communications network (paragraph 27, where network devices may be computer hosts, and paragraph 30, "According to one embodiment, the policies relevant to a particular network device 24, 26, 28 are selected based on a role assigned to the device" and paragraph 35, "A rule type may organize policies into role policies", *where the role (policy) [i.e. service abstraction layer] is replaced by Azarmi's feature set [i.e. role abstraction layer]*).

6. Claim 26 is rejected under 35 U.S.C. 103(a) as being unpatentable over See.

**Regarding claim 26**, See describes a system of controlling usage of network resources on a communication network, comprising:

(A) creating one or more packet rules (policy rules) for analyzing packets received at one or more devices of the communications network, each rule including a condition and action to be taken if a packet received at a device satisfies the condition (fig. 4 and paragraph 35);

(B) creating one or more service abstractions (policy groups), each service abstraction representing a named set of one or more of the packet rules (paragraph 35,

"According to one embodiment, the policy rules are organized into policy groups based on a rule type 52".

See lacks describing that a computer program product to perform the above-mention process, comprising:

a computer readable medium and computer readable signals stored on the computer readable medium that define instructions that, as a result of being executed by a computer, instruct the computer to perform the process.

The examiner takes official notice that the system of See may be implemented using a computer comprising a readable medium and a program with instructions which executes the process. The motivation being that such implementation using a [generic] computer may be more economical and faster to develop than via a customized hardware system.

***Conclusion***

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure: Engel (6,519,636) and Li (6,567,408).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Warner Wong whose telephone number is 571-272-8197. The examiner can normally be reached on 5:30AM - 2:00PM, M-F.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Chieh Fan can be reached on 571-272-3042. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Warner Wong
Examiner
Art Unit 2668

WW

CHIEH M. FAN
SUPERVISORY PATENT EXAMINER